to further requests for access to sensitive, proprietary or classified information or technology, are to be reported to designated security officers. Reports of such contacts are to be forwarded by the designated security officer to the Departmental Director of Security for appropriate action and coordination.

Subpart E—Implementation and Review

§ 2.38 Departmental management.

(a) The Assistant Secretary (Management) shall:

(1) Enforce the Order, the Directive and this regulation, and establish, coordinate and maintain active training, orientation and inspection programs for employees concerned with classified information.

(2) Review suggestions and complaints regarding the administration of this regulation.

(b) Pursuant to Treasury Directive 71–08, ''Delegation of Authority Concerning Physical Security Programs'', the Departmental Director of Security shall:

(1) Review all bureau implementing regulations prior to publication and shall require any regulation to be changed, if it is not consistent with the Order, the Directive or this regulation.

(2) Have the authority to conduct onsite reviews of bureau physical security programs and information security programs as they pertain to each Treasury bureau and to require such reports, information and assistance as may be necessary, and

(3) Serve as the principal advisor to the Assistant Secretary (Management) with respect to Treasury physical and information security programs.

§ 2.39 Bureau administration.

Each Treasury bureau and the Departmental Offices shall designate, in writing to the Departmental Director of Security, an officer or official to direct, coordinate and administer its physical security and information security programs which shall include active oversight to ensure effective implementation of the Order, the Directive, this regulation. Bureaus and the Departmental Offices shall revise their existing implementing regulation on national security information to ensure conformance with this regulation. Time frames for bureau and Departmental Offices implementation shall be established by the Departmental Director of Security.

§ 2.40 Emergency planning [4.1(b)].

Each Treasury bureau and the Departmental Offices shall develop plans for the protection, removal, or destruction of classified information in case of fire, natural disaster, civil disturbance, or possible enemy action. These plans shall include the disposition of classified information located in foreign countries.

§ 2.41 Emergency authority [4.1(b)].

The Secretary of the Treasury may prescribe by regulation special provisions for the dissemination, transmittal, destruction, and safeguarding of national security information during combat or other emergency situations which pose an imminent threat to national security information.

§ 2.42 Security education [5.3(a)].

Each Treasury bureau that creates, processes or handles national secutity information, including the Departmental Offices, is required to establish a security education program. The program shall be sufficient to familiarize all necessary personnel with the provisions of the Order, the Directive, this regulation and any other implementing directives and regulations to impress upon them their individual security responsibilities. The program shall also provide for initial, refresher, and termination briefings.

(a) *Briefing of Employees.* All new employees concerned with classified information shall be afforded a security briefing regarding the Order, the Directive and this regulation and sign a security agreement as required in §2.22(c). Employees concerned with sensitive compartmented information shall be required to read and also sign a security agreement. Copies of applicable laws and pertinent security regulations setting forth the procedures for the protection and disclosure of classified information shall be available for all new employees afforded a security

briefing. All employees given a security briefing shall be required to sign a TD F 71–01.16 (Physical Security Orientation Acknowledgment) which shall be maintained on file as determined by respective office or bureau security officials.

(b) [Reserved]

Subpart F—General Provisions

§2.43 Definitions [6.1].

(a) *Authorized Person.* Those individuals who have a ''need-to-know'' the classified information involved and have been cleared for the receipt of such information. Responsibility for determining whether individuals' duties require that they possess, or have access to, any classified information and whether they are authorized to receive it rests on the individual who has possession, knowledge, or control of the information involved, and not on the prospective recipients.

(b) *Compromise.* The loss of security enabling unauthorized access to classified information. Affected information or material is not automatically declassified.

(c) *Confidential Source.* Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence.

(d) *Declassification.* The determination that particular classified information no longer requires protection against unauthorized disclosure in the interest of national security. Such determination shall be by specific action or occur automatically after the lapse of a requisite period of time or the occurrence of a specified event. If such determination is by specific action, the information or material shall be so marked with the new designation.

(e) *Derivative Classification.* A determination that information is, in substance, the same as informaiton that is currently classified and a designation of the level of classification.

(f) *Designated Countries of Concern.* For purposes of National Security Decision Directive 197 reporting: Afghanistan, Albania, Angola, Bulgaria, Cambodia (Kampuchea), the People's Republic of China (Communist China), Cuba, Czechoslovakia, Ethiopia, East Germany (German Democratic Republic including the Soviet sector of Berlin), Hungary, Iran, Iraq, Laos, Libya, Mongolian People's Republic (Outer Mongolia), Nicaragua, North Korea, Palestine Liberation Organization, Poland, Romania, South Africa, South Yemen, Syria, Taiwan, Union of Soviet Socialist Republics (Russia), Vietnam and Yugoslavia.

(g) *Document.* Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed material; data processing cards and tapes; maps, charts; painting; drawings; engravings; sketches; working notes and papers; reproductions of such things by any means or process; and sound, voice, or electronic recordings in any form.

(h) *Foreign Government Information.* (1) Information provided by a foreign government or governments, an international organization of governments, or any elements thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

(2) Information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

(i) *Information.* Any data or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.

(j) *Information Security.* The administrative policies and procedures for identifying, controlling, and safeguarding from unauthorized disclosure, information the protection of which is authorized by Executive Order or statute.

(k) *Intelligence Activity.* An activity that an agency within the Intelligence Community is authorized to conduct pursuant to Executive Order 12333.